

Application #09/993,899
Amendment dated December 27, 2005

Amendments to the claims:

1. (Currently Amended) A method for accessing cryptographic material comprising the steps of:

- 5 creating cryptographic material, by a first Cryptographic-related application programming interface ("API") associated with a first cryptographic standard, in response to a request by a first application compatible with the first Cryptographic-related API; and
- creating a supplemental aspect of the cryptographic material by a
- 10 supplemental method for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API associated with a second cryptographic standard so that the cryptographic material is accessible for a second application by the second Cryptographic-related
- 15 API.

2. (Original) The method of claim 1, wherein the step of creating cryptographic material comprises
- creating a certificate or private key, and the step of creating the
- 20 supplemental aspect of the cryptographic material comprises the steps of:
- deriving a key container name from the certificate or private key;
- and
- determining whether the key container already exists.

Application #09/993,899
Amendment dated December 27, 2005

3. (Original) The method of claim 2, wherein the step of deriving a key container name comprises the steps of:

creating a hash responsive to material from the certificate or
5 private key; and
encoding the hash.

4. (Original) The method of claim 2, wherein the step of creating a certificate or private key comprises creating the private key and wherein if
10 the key container already exists for the key, the step of creating the supplemental aspect of the cryptographic material comprises the steps of:

determining whether the key container contains a certificate;
associating the private key as a member of a key pair associated
with the certificate, if the key container contains a certificate; and
15 associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate.

5. (Original) The method of claim 2, wherein the step of creating a certificate or private key comprises creating the certificate, and the step of
20 creating the supplemental aspect of the cryptographic material comprises the steps of:

extracting a key specification from the certificate; and

Application #09/993,899
Amendment dated December 27, 2005

associating the certificate with a key pair under the extracted key specification.

6. (Original) The method of claim 2, wherein the step of creating a
5 certificate or private key comprises creating the certificate, and wherein if
the key container already exists for the certificate the step of creating the
supplemental aspect of the cryptographic material comprises the steps of:
determining whether the key container has a private key; and
associating the private key with a same key pair as the certificate, if
10 the key container has the private key.

7. (Original) The method of claim 2, wherein the step of creating a
certificate or private key comprises creating the certificate, and the step of
creating the supplemental aspect of the cryptographic material comprises
15 the step of:
creating a public key from information in the certificate.

8. (Original) The method of claim 1, wherein the first
Cryptographic-related API is one from the set of PKCS #11, CryptoAPI,
20 and CDSA compatible API's, and the second Cryptographic-related API is
not the same API as the first and is also one from the set of PKCS #11,
CryptoAPI and CDSA compatible API's.

Application #09/993,899
Amendment dated December 27, 2005

9. (Original) The method of claim 1, wherein the first
Cryptographic-related API uses a certain term and the second
Cryptographic-related API has a corresponding term, and wherein
creating the supplemental aspect comprises creating material indicating a
5 cross-reference between the terms.

10. (Currently Amended) A computer program product for
accessing cryptographic material comprising:

first instructions for creating cryptographic material, by a first
10 Cryptographic-related application programming interface ("API")
associated with a first cryptographic standard, in response to a request by
a first application compatible with the first Cryptographic-related API;
and

second instructions for creating a supplemental aspect of the
15 cryptographic material for the first cryptographic API, wherein the
supplemental aspect includes information for rendering the cryptographic
material compatible with a second Cryptographic-related API associated
with a second cryptographic standard so the cryptographic material is
accessible for a second application by the second Cryptographic-related
20 API.

Application #09/993,899
Amendment dated December 27, 2005

11. (Original) The computer program product of claim 10, wherein the first instructions comprise instructions for creating a certificate or private key, and the second instructions comprise:

instructions for deriving a key container name from the certificate
5 or private key; and
instructions for determining whether the key container already exists.

12. (Original) The computer program product of claim 11, wherein
10 the instructions for deriving a key container name comprise:

instructions for creating a hash responsive to material from the certificate or private key; and
instructions for encoding the hash.

15 13. (Original) The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the private key, and the second instructions comprise:

instructions for determining whether the key container contains a
20 certificate, if the key container does already exist for the key;
instructions for associating the private key as a member of a key pair associated with the certificate, if the key container contains a certificate; and

Application #09/993,899
Amendment dated December 27, 2005

instructions for associating the private key as a member of a key pair having a default key specification, if the key container does not contain a certificate.

- 5 14. (Original) The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the certificate, and the second instructions comprise:

instructions for extracting a key specification from the certificate;

10 and

instructions for associating the certificate with a key pair under the extracted key specification.

- 15 15. (Currently Amended) The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the certificate, and wherein the second instructions comprise:

determining whether the key container has a private key, if a key container does already exist for the certificate; and

- 20 associating the private key with a same key pair as the certificate, if the key container has the private key.

Application #09/993,899
Amendment dated December 27, 2005

16. (Original) The computer program product of claim 11, wherein the instructions for creating a certificate or private key comprise instructions for creating the certificate, and wherein the second instructions comprise:

5 instructions for creating a public key from information in the certificate.

17. (Original) The computer program product of claim 10, wherein the first Cryptographic-related API is one from the set of PKCS #11, 10 CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is a different API than the first Cryptographic-related API and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's.

15 18. (Original) The computer program product of claim 10, wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein the instructions for creating the supplemental aspect comprise instructions for creating material indicating a cross-reference between the terms.

20

19. (Currently Amended) An apparatus for accessing cryptographic material comprising:

a processor; and

Page 12 of 21

A43_2_Amend_10-02y.doc

Application #09/993,899
Amendment dated December 27, 2005

a memory coupled to the processor for storing instructions for controlling the processor, wherein the processor is operative with the instructions to perform the steps of:

5 a) creating cryptographic material, by a first Cryptographic-related application programming interface ("API") associated with a first cryptographic standard, in response to a request by a first application compatible with the first Cryptographic-related API; and

10 b) creating a supplemental aspect of the cryptographic material by a supplemental method for the first cryptographic API, wherein the supplemental aspect includes information for rendering the cryptographic material compatible with a second Cryptographic-related API associated with a second cryptographic standard so that the cryptographic material is accessible for a second application by
15 the second Cryptographic-related API.

20. (Original) The apparatus of claim 19, wherein step a) comprises creating a certificate or private key, and step b) comprises the steps of:

20 deriving a key container name from the certificate or private key; and
determining whether the key container already exists.

Application #09/993,899
Amendment dated December 27, 2005

21. (Original) The apparatus of claim 20, wherein the step of
deriving a key container name comprises the steps of:

creating a hash responsive to material from the certificate or
private key; and

5 encoding the hash.

22. (Original) The apparatus of claim 20, wherein the step of
creating a certificate or private key comprises creating the private key and
wherein if the key container already exists for the key, step b) comprises

10 the steps of:

determining whether the key container contains a certificate;

associating the private key as a member of a key pair associated
with the certificate, if the key container contains a certificate; and

15 associating the private key as a member of a key pair having a
default key specification, if the key container does not contain a certificate.

23. (Original) The apparatus of claim 20, wherein the step of
creating a certificate or private key comprises creating the certificate, and
step b) comprises the steps of:

20 extracting a key specification from the certificate; and

associating the certificate with a key pair under the extracted key
specification.

Application #09/993,899
Amendment dated December 27, 2005

24. (Original) The apparatus of claim 20, wherein the step of creating a certificate or private key comprises creating the certificate, and wherein if the key container already exists for the certificate step b) comprises the steps of:

- 5 determining whether the key container has a private key; and
 associating the private key with a same key pair as the certificate, if the key container has the private key.

25. (Original) The apparatus of claim 20, wherein the step of
10 creating a certificate or private key comprises creating the certificate, and step b) comprises the step of:

 creating a public key from information in the certificate.

26. (Original) The apparatus of claim 19, wherein the first
15 Cryptographic-related API is one from the set of PKCS #11, CryptoAPI, and CDSA compatible API's, and the second Cryptographic-related API is not the same API as the first and is also one from the set of PKCS #11, CryptoAPI and CDSA compatible API's.

20 27. (Currently Amended) The apparatus of claim 19, wherein the first Cryptographic-related API uses a certain term and the second Cryptographic-related API has a corresponding term, and wherein

Application #09/993,899
Amendment dated December 27, 2005

creating the supplemental aspect comprises creating material indicating a
cross-reference between the terms.